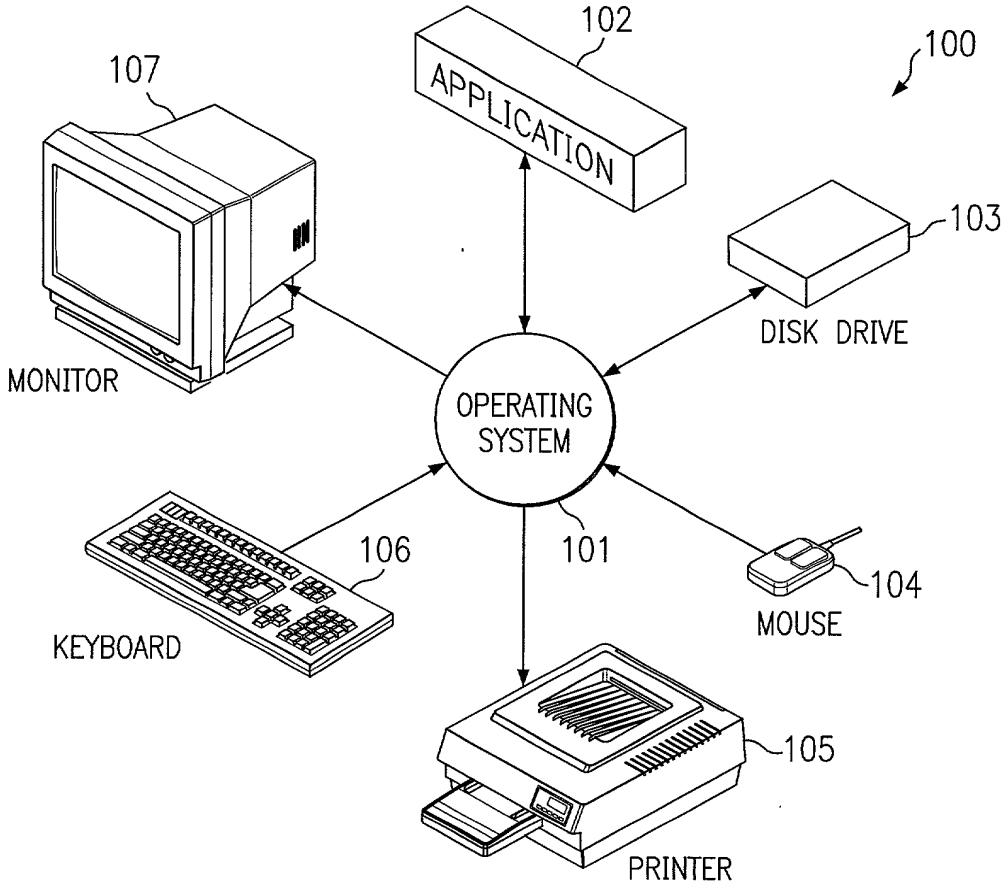

FIG. 1
(PRIOR ART)

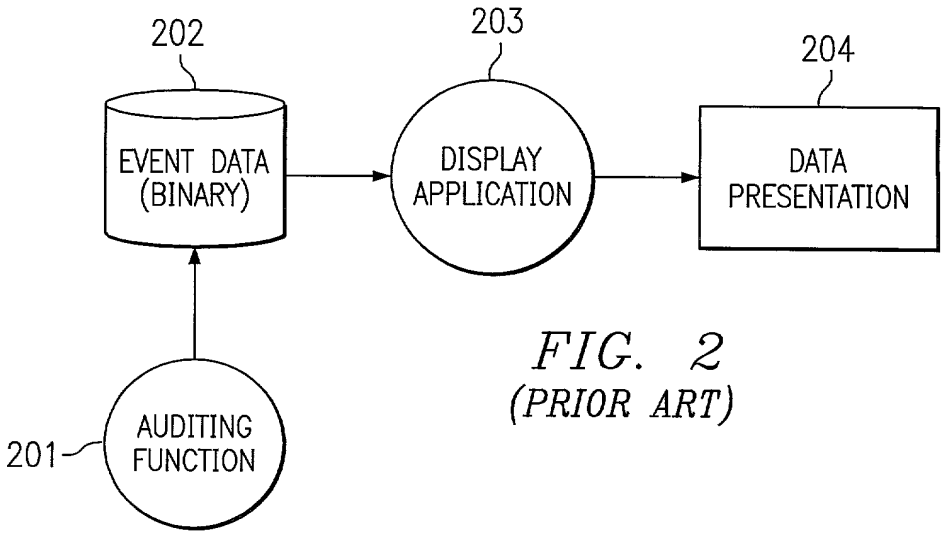

FIG. 2
(PRIOR ART)

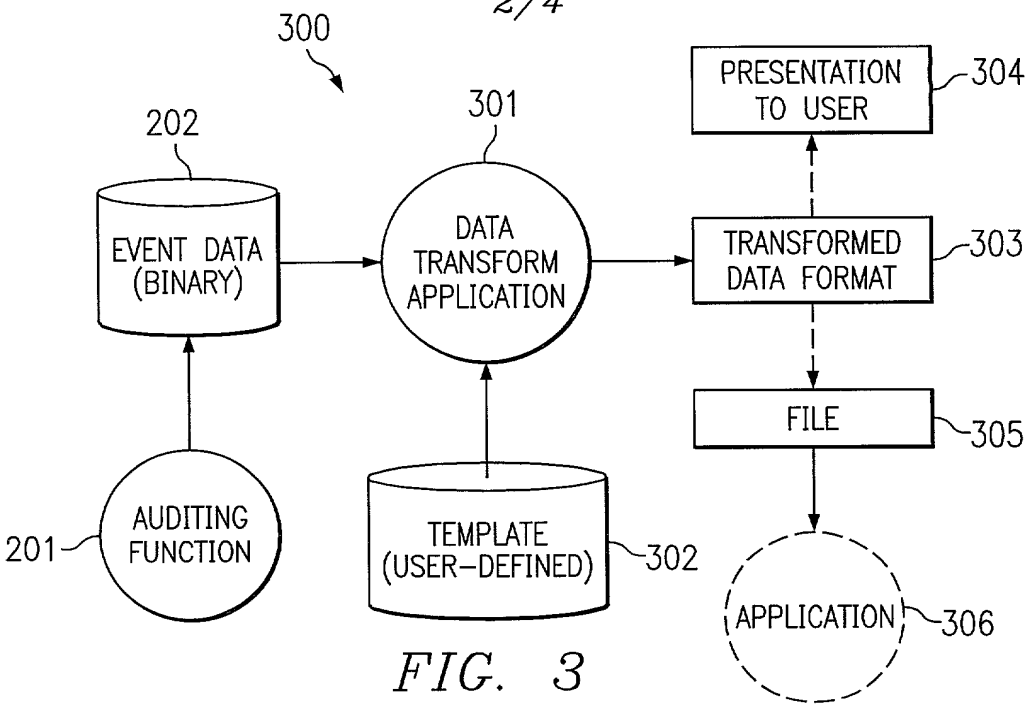

FIG. 3

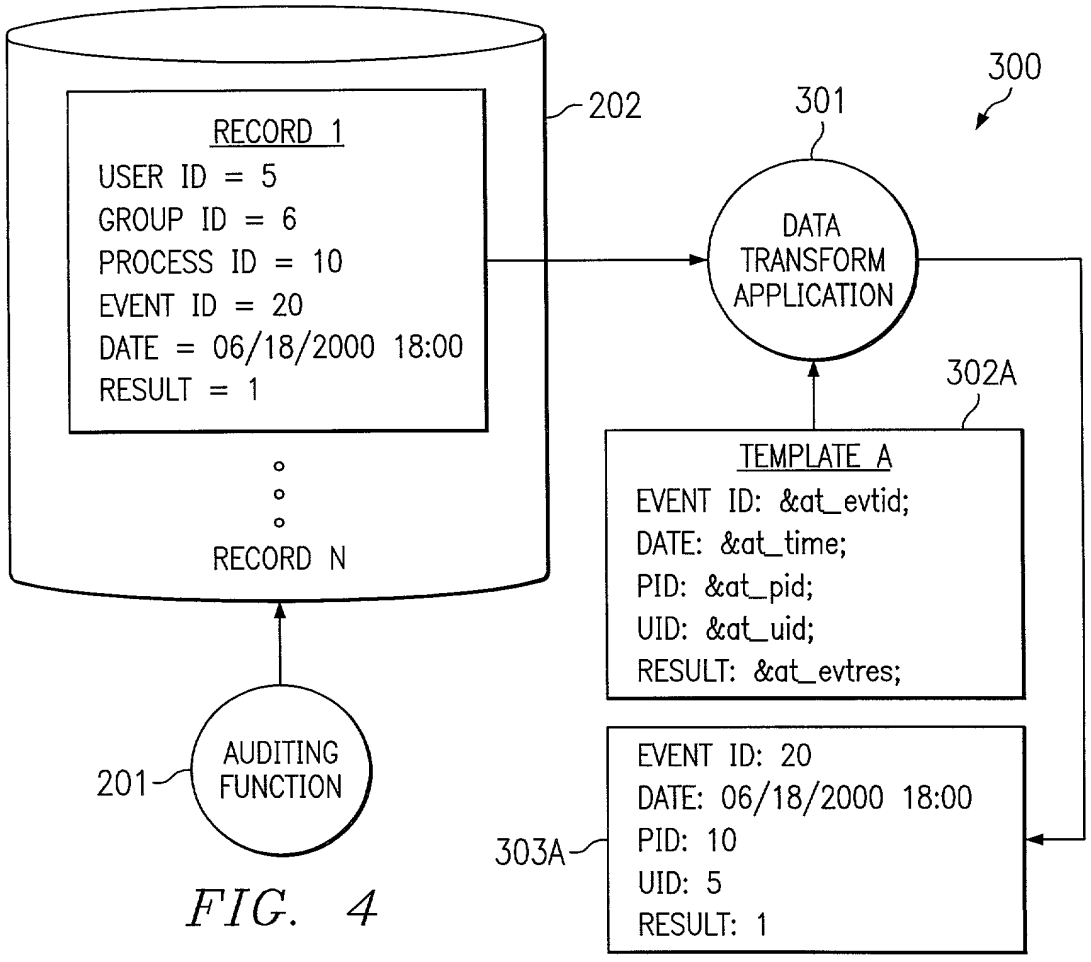

FIG. 4

09699351 .062501

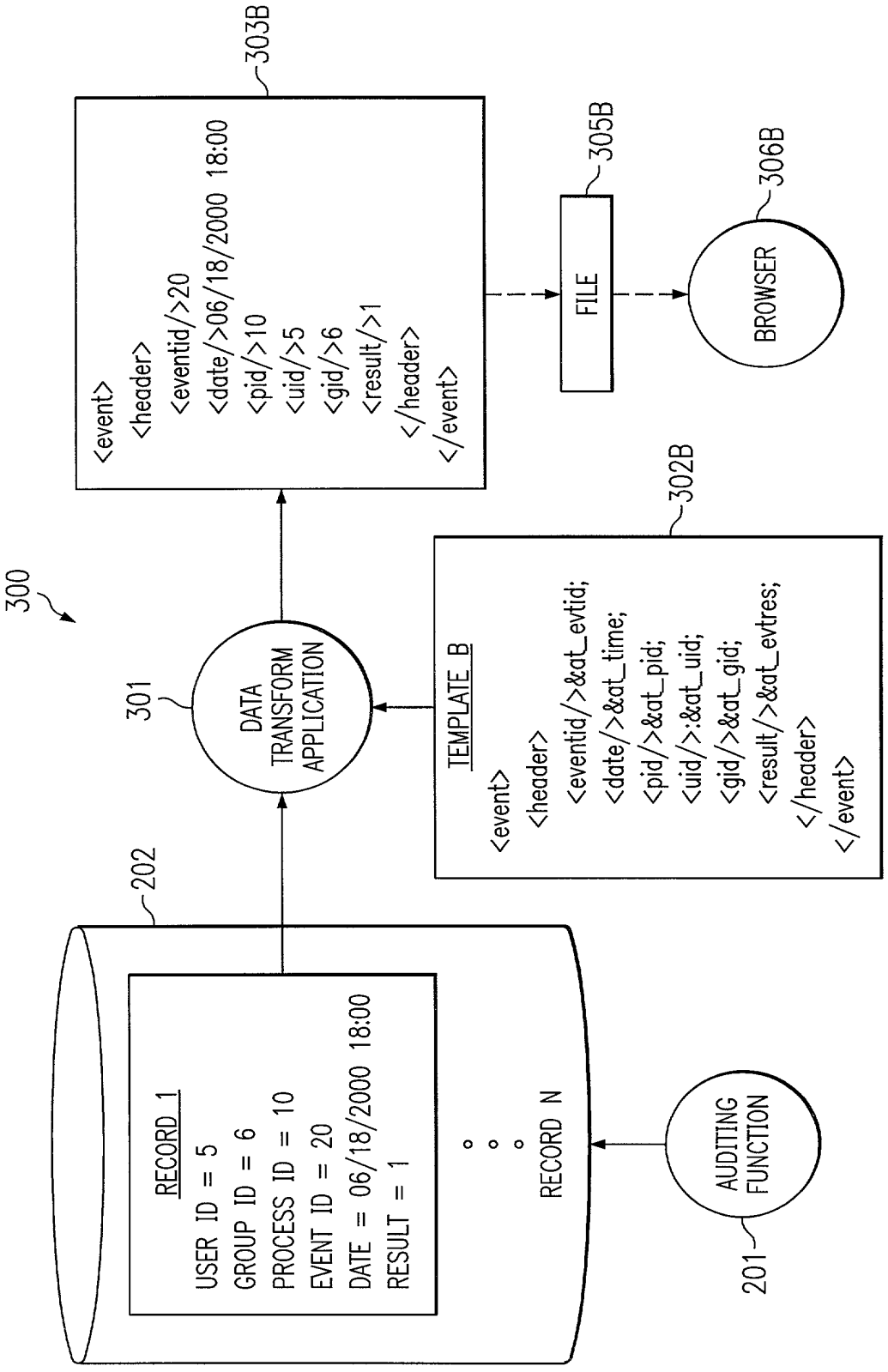
300
202
RECORD 1
USER ID = 5
GROUP ID = 6
PROCESS ID = 10
EVENT ID = 20
DATE = 06/18/2000 18:00
RESULT = 1
RECORD N
201
AUDITING FUNCTION
301
DATA TRANSFORM APPLICATION
302B
TEMPLATE B
<event>
<header>
<eventid/>&at_evtid;
<date/>&at_time;
<pid/>&at_pid;
<uid/>:&at_uid;
<gid/>&at_gid;
<result/>&at_evtres;
</header>
</event>
303B
<event>
<header>
<eventid/>20
<date/>06/18/2000 18:00
<pid/>10
<uid/>5
<gid/>6
<result/>1
</header>
</event>
305B
FILE
306B
BROWSER

FIG. 5

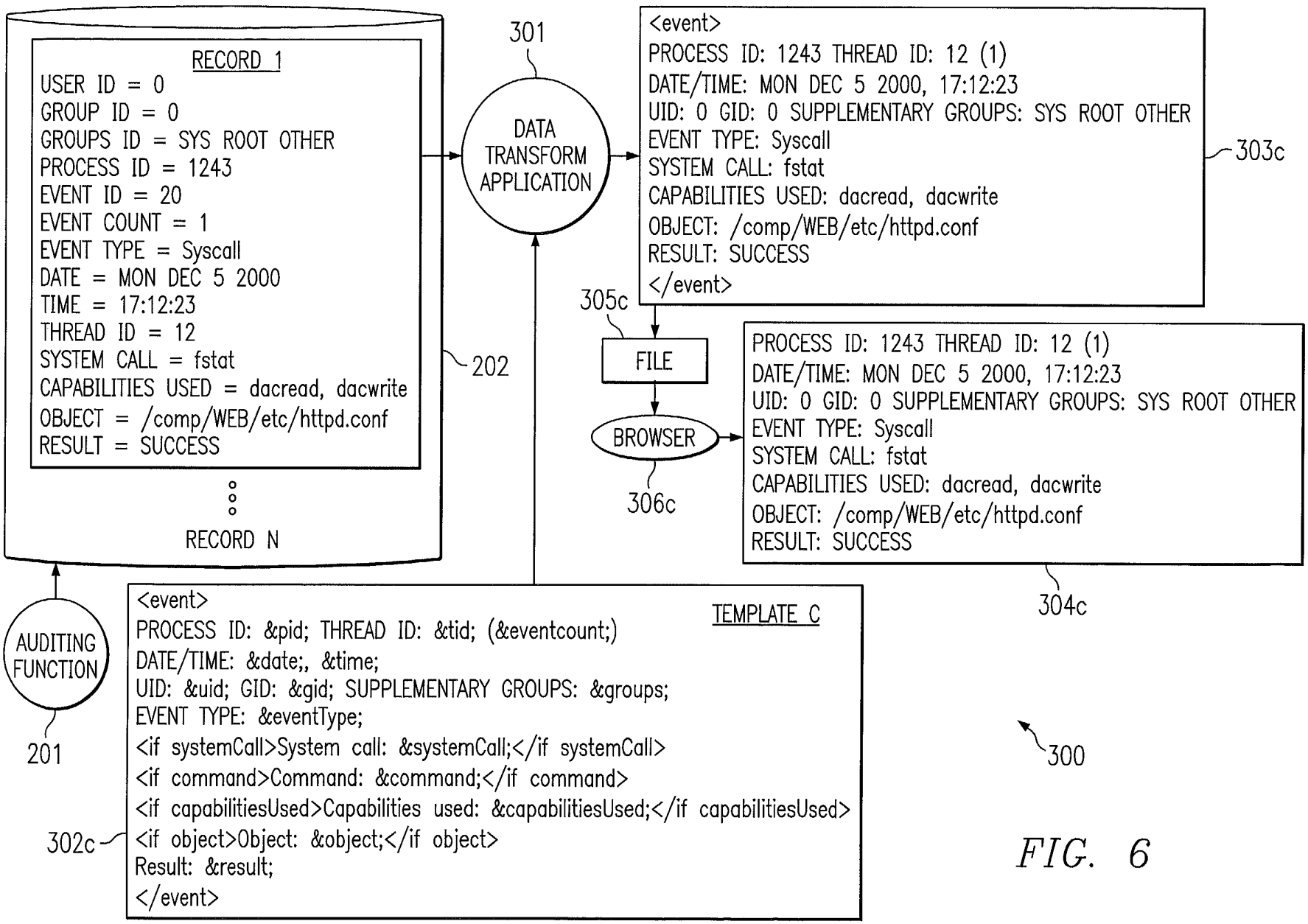
RECORD 1
USER ID = 0
GROUP ID = 0
GROUPS ID = SYS ROOT OTHER
PROCESS ID = 1243
EVENT ID = 20
EVENT COUNT = 1
EVENT TYPE = Syscall
DATE = MON DEC 5 2000
TIME = 17:12:23
THREAD ID = 12
SYSTEM CALL = fstat
CAPABILITIES USED = dacread, dacwrite
OBJECT = /comp/WEB/etc/httpd.conf
RESULT = SUCCESS
RECORD N
202
301
DATA TRANSFORM APPLICATION
<event>
PROCESS ID: 1243 THREAD ID: 12 (1)
DATE/TIME: MON DEC 5 2000, 17:12:23
UID: 0 GID: 0 SUPPLEMENTARY GROUPS: SYS ROOT OTHER
EVENT TYPE: Syscall
SYSTEM CALL: fstat
CAPABILITIES USED: dacread, dacwrite
OBJECT: /comp/WEB/etc/httpd.conf
RESULT: SUCCESS
</event>
303c
305c
FILE
BROWSER
306c
PROCESS ID: 1243 THREAD ID: 12 (1)
DATE/TIME: MON DEC 5 2000, 17:12:23
UID: 0 GID: 0 SUPPLEMENTARY GROUPS: SYS ROOT OTHER
EVENT TYPE: Syscall
SYSTEM CALL: fstat
CAPABILITIES USED: dacread, dacwrite
OBJECT: /comp/WEB/etc/httpd.conf
RESULT: SUCCESS
304c
AUDITING FUNCTION
201
TEMPLATE C
<event>
PROCESS ID: &pid; THREAD ID: &tid; (&eventcount;)
DATE/TIME: &date;, &time;
UID: &uid; GID: &gid; SUPPLEMENTARY GROUPS: &groups;
EVENT TYPE: &eventType;
<if systemCall>System call: &systemCall;</if systemCall>
<if command>Command: &command;</if command>
<if capabilitiesUsed>Capabilities used: &capabilitiesUsed;</if capabilitiesUsed>
<if object>Object: &object;</if object>
Result: &result;
</event>
302c
300

FIG. 6